
دار المنظومة
DAR ALMANDUMAH
الرواد في قواعد المعلومات العربية

الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الإلكترونية [1]

اللواء الدكتور محمد حسن السراء [2]
أستاذ مساعد بقسم العلوم الشرطية بكلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية - السعودية

مستخلص

سعت هذه الدراسة إلى تلمس طبيعة الجرائم الإلكترونية التي لا تبدو في كثير من الحالات غامضة ومعقدة فحسب ، بل تمثل تحدياً هائلاً يستدعي سرعة التأهب نحو نقلة علمية وتقنية دائبة تحققها باذات مجالات الشرطة والقضاء والنيابة ، وسعت هذه الدراسة أيضاً إلى إبراز طبيعة هذه الجرائم وصورها المختلفة التي باتت تشكل أهم جرائم هذا العصر وأعقدها خاصة في المجالات الأمنية لحماية المواقع الالكترونية والبيانات الشخصية ومنع الاعتداء على الأموال الالكترونية وحماية التوقيع الالكتروني وحماية المستهلك الالكتروني ، بل والاقتصاد الوطني وغيرها. وتناول البحث بعض المخاطر التي تواجه نظام المعلومات وكيفية تحسين التدابير الأمنية والوقائية مع مراعاة حماية الخصوصية لدى أداء المهام الأمنية ، وإبراز بعض الجهود الوقائية الوطنية. من هنا فإن تطبيق برامج تدريبية والأخذ بالتجارب الناجحة للتعامل مع الأدلة الجنائية ومواكبة مستجداتها هو المعول عليه الارتقاء بالتحقيق وكافة الإجراءات الإجرائية المطلوبة في هذه الجرائم وجمع الاستدلالات وهو ما يهدف إليه أيضا هذا البحث في أحد محاوره المهمة. وإذا كان هذا الحقل يتطلب اليوم الاستعانة الكاملة بخبراء الحاسوب لكشف غموض الأدلة الرقمية فإن استقلالية الشرطة والنيابة التعامل مع هذه الأدلة أضحى ضرورة مهنية. وخلصت هذه الدراسة إلى نتائج وتوصيات عدة من أهمها: إن مخاطر تصاعد وتيرة الجرائم الإلكترونية وتداعياتها الاقتصادية والجنائية والأخلاقية يجعل هذه القضية من كبرى القضايا الأمنية في وقتنا الحاضر ، فعليه نوصي بدراسة هذه الظاهرة دراسة مستفيضة من قبل الجهات المعنية كافة. هناك مواكبة حثيثة لاقتناء التقنية المعلوماتية في المملكة والاستفادة منها تواكبها أيضا جهود وقائية من الجرائم تتمثل في صدور الأنظمة والتشريعات والدور المنوط بمدينة الملك عبد العزيز للعلوم والتقنية. في مجال التحقيق في الجرائم الالكترونية هناك بعض المعوقات التي تعترض الأداء المهني التقني الرفيع. السعي إلى الاستفادة من الكفاءات العلمية والتقنية المتميزة في مجالات الأمن والادعاء العام والقضاء. تعميم مقرر مادة التحقيق في الجرائم الالكترونية وتشريعاتها "في المدارس والكليات الأمنية" العربية. بث الوعي الأمني لدى الجمهور عن مخاطر الجريمة الالكترونية. انتقاء ذوي المواهب والقدرات التقنية العالية العمل في مجالات التحقيقات في الجرائم الإلكترونية.

مفردات البحث :

الجرائم الإلكترونية — المواقع الإلكترونية — الأموال الإلكترونية — الأدلة الإلكترونية — المعامل الإلكترونية.

1- ورد هذا البحث للدورية في سبتمبر 2011م وقيد تحت رقم (2012/7م جديد) ، وأحيل للتحكيم في أكتوبر 2011م وأجيز للنشر في فبراير 2012م.

2- حصل اللواء الدكتور محمد حسن السراء على درجة الدكتوراه في التخطيط والتنظيم والسياسة الإدارية من جامعة كاليفورنيا بالولايات المتحدة الأمريكية 1990م وعمل في كلية الملك فهد الأمنية قبل أن ينتقل للعمل في جامعة نايف العربية للعلوم الأمنية أستاذاً مساعداً بقسم العلوم الشرطية وله العديد من البحوث والدراسات المنشورة.

المبحث الأول
مشكلة الدراسة وتساؤلاتها

لا شك أن لهذا الربط والثنائية بين تقنية المعلومات والأمن الوطني دلالات علمية وأمنية قيمة ، إذ يدعم هذا التوجه كافة الموضوعات والمحاور والقضايا المطروحة حول آثار وأبعاد هذه التقنيات وانعكاساتها المختلفة خاصة في المجالات الاستراتيجية والأمنية.

وتسعى هذه الورقة إلى تلمس طبيعة الجرائم الالكترونية التي لا تبدو في كثير من الحالات غامضة ومعقدة فحسب ، بل تمثل تحدياً هائلاً يستدعي سرعة التأهب نحو نقلة علمية وتقنية دائبة تحققها بالذات مجالات الشرطة والقضاء والنيابة ، ثم إن هناك قلقاً يراود الساحة الأمنية يتمثل في أن كثيراً من الميادين كالتشريعات والقوانين والأنظمة وغيرها أخذت تحرز تقدماً ملحوظا وإنجازات في تنظيم وضبط هذه الجرائم ، بينما أجهزة الشرطة المعنية لا تزال في معظم الحالات تواجه هذه الأنماط الإجرامية البالغة التعقيد بأدوات تتضاءل دون براعة الجريمة الإلكترونية وأضرارها الفادحة.

وتسعى هذه الورقة أيضاً إلى إبراز طبيعة هذه الجرائم وصورها المختلفة التي باتت تشكل أهم جرائم هذا العصر وأعقدها خاصة في المجالات الأمنية لحماية المواقع الالكترونية والبيانات الشخصية ومنع الاعتداء على الأموال الالكترونية وحماية التوقيع الالكتروني وحماية المستهلك الالكتروني ، بل والاقتصاد الوطني وغيرها.

كما تبرز في هذه البيئة الالكترونية المخاطر الشائعة في الآونة الأخيرة ومنها الهجمات الحاقدة والتجسس الحكومي والتجسس الصناعي التي تجعل قواعد المعلومات في المواقع العسكرية والاستراتيجية واختراقها هدفاً يجب أن ينصرف إليه البحث العلمي وجهود الباحثين والمسئولين على حد سواء لحماية الوطن ومقدراته.

ويتناول البحث كذلك بعض المخاطر التي تواجه نظام المعلومات وكيفية تحسين التدابير الأمنية والوقائية مع مراعاة حماية الخصوصية لدى أداء المهام الأمنية ، وإبراز بعض الجهود الوقائية الوطنية.

من هنا فإن تطبيق برامج تدريبية والأخذ بالتجارب الناجحة للتعامل مع الأدلة الجنائية ومواكبة مستجداتها هو المعول عليه للارتقاء بالتحقيق وكافة الإجراءات الإجرائية المطلوبة في هذه الجرائم وجمع الاستدلالات وهو ما يهدف إليه أيضا هذا البحث في أحد محاوره المهمة ، وإذا كان هذا الحقل يتطلب اليوم الاستعانة الكاملة تقريباً بخبراء الحاسوب لكشف غموض الأدلة فإن استقلالية رجال الشرطة والنيابة للتعامل مع هذه الأدلة والجرائم تصبح ضرورة مهنية ومعرفية يجب توفيرها في ظل خطة تدريبية الكترونية طموحة.

1- **مشكلة الدراسة**

تتصف الجرائم الإلكترونية بالحداثة وسرعة التنفيذ وسهولة الإخفاء ودقة محو آثارها ، لذا تسعى الدراسة إلى البحث في الوسائل الحديثة في مجال التحقيق والتحري والضبط وبيان الصعوبات الفنية والمعوقات التشريعية والأمنية المختلفة التي تكتنف هذا النمط الجديد من الجرائم وما يتطلبه من تطوير متسارع لأساليب التحقيق الجنائي وإجراءاته بصورة فعالة تنهض بالتأهيل الفني الرفيع المنشود لرجال الشرطة **والمهارة المتقدمة** في التعامل مع الملفات والجرائم والأجهزة ، أملاً في إيجاد مراكز عربية ووطنية متخصصة في هذه الجرائم ؛ لأن النقص في الكادر الأمني في هذا المجال يفضي إلى عجز خطير عن مواكبة هذه الجرائم الإلكترونية الخطيرة. ثم إن التحقيق هنا ، وغيره من المهام الأمنية في بيئة إلكترونية تستدعي التعاطي معها بلغتها وحيثياتها المعقدة.

وتتمثل مشكلة الدراسة في التساؤل الرئيس التالي: *ما الأساليب والمهارات الحديثة المطلوبة في مجال التحقيق في الجرائم الإلكترونية؟*

2- **تساؤلات الدراسة:**

من أهم التساؤلات التي تبرزها الدراسة ما يلي:

1- وضعت الجرائم الإلكترونية عبئاً هائلاً بالغ التعقيد على المسئولية الأمنية ومهامها الراهنة بحيث لا يتأتى لرجل الأمن التعامل معها إلا ببراعة ومهارة.

2- أظهرت هذه المشكلة فجأة عدم التكافؤ بين معطيات التقنية المعلوماتية السريعة التطور وتداعياتها الخطيرة على أنماط الجريمة وبين وتيرة الأدلة الجنائية المألوفة للأجهزة الأمنية في أساليب التأهيل والتحديث ، ما يشجع اليوم على تفاقم الجرائم الإلكترونية في مجتمعاتنا.

3- لا يكاد يمتلك التحقيق من الأدوات وأدلة الإثبات والوسائل العلمية ما يمكنه من التعامل مع محيط شاسع من الجرائم المعلوماتية ببرامجها المعقدة وشباكها الدقيقة وأجهزتها المختلفة.

4- حاجة التحقيق الجنائي للجرائم الإلكترونية الماسة إلى مهارات متقدمة تستدعي العديد من المقومات الفنية والعلمية والإدارية والقانونية وغيرها ، لإعداد رجال الأمن في هذا التخصص الدقيق.

3- **أهمية الدراسة:**

تتمثل أهمية هذه الدراسة في النقاط التالية:

- تسليط الضوء على أبعاد الأنشطة الإجرامية المنفذة في حقل الجرائم المعلوماتية وجرائم الإنترنت ومخاطرها الاقتصادية والاجتماعية والتربوية.
- الاهتمام بالجرائم المعلوماتية والبحث في التدابير العلمية والفنية لاكتشافها والسيطرة عليها.
- العناية بضبط الجرائم المعلوماتية وبتمليك رجال التحقيق تقنيات وأدوات ترتقي بهم إلى مصاف المواكبة المتطورة في ميادين التدريب والتأهيل.
- الإسهام في الوعي الأمني للحد من هذه الجرائم ولمساعدة المتضررين في الإبلاغ للجهات المختصة لضبط الأدلة.

- عرض بعض الملامح لأنواع مستجدة من التحقيقات الجنائيـــة علـــى ضـــوء هـــذه المتغيرات الطارئة في مسارح الجريمة وأساليب المجرمين.

4- منهجية الدراسة:

تعتمد الدراسة على المنهج الوصفي التحليلي ، ويقوم على ما يلي:

- العناية بتناول كافة المحاور الرئيسة سواء ما يتسم بالصـــعوبات والمعوقـــات فـــي الجرائم المعلوماتية وما يتجسد أمام التحقيق من تحديات وكيفية الارتقاء بـــإجراءات التحقيق.
- يعنى البحث بالوقوف على بعض التجارب والتطبيقات لدى بعض الدول المتقدمة.
- وضع تصور علمي ومهني للنهوض بالتحقيقات الجنائية في جرائم المعلوماتية.

5- مصطلحات الدراسة:

جرائم الحاسب الآلي والإنترنت (Computer Crime) :

هي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة وغيـــر مباشـــرة كوسيلة أو أهداف لتنفيذ الفعل الإجرامي المقصود.

جرائم عبر الكمبيوتر (Cyber) :

هي الجرائم ذات الصلة بالكمبيوتر والإنترنت والشبكة المعلوماتية تجتمع فيها جرائم الشبكة العالمية (Welcome Computer) (مثل الاحتيال ، غسل الأموال ، المخدرات) ، وكذلك جرائم الكمبيوتر (Cumber) (مثل الإضرار بقواعد البيانات (DATA BASES) أو المكونات المادية (Hardware) أو المكونات المعنوية (Software).

الجريمة المعلوماتية (Informatics Crime) :

للجريمة المعلوماتية مسميات كثيرة منها: جريمة الكمبيوتر والإنترنـــت ، الجريمـــة الإلكترونية ، الجرائم المستحدثة. وهذه التسميات ناشئة من اخـــتلاف التعريـــف القـــانوني

والفني للمصطلح. وكذلك سوء استخدام الحاسبات (Computer Abuse) ، والجرائم الرقمية (Digital Crime) ، وتتميز هذه الجرائم بصعوبة كشفها نظراً لإمكانية ارتكابها من مسافات بعيدة ، ولقدرة الجاني في تدمير الأدلة عليها في أقل من الثانية الواحدة وكونها لا تترك أي أثر مرئي.

مهارات التحقيق (Investigation Skills):

تتمثل في الإجراءات القانونية والإدارية والفنية التي تتخذها سلطة رسمية ذات اختصاص بقصد كشف الجريمة والتعرف على الجناة والمتضررين من الجريمة وجمع الأدلة التي تحقق العدالة الجنائية , ويتسم هذا النوع من التحقيق بالذات بالبراعة والمواهب والقدرات الفذّة.

6- العمل الأمني والجريمة الالكترونية :

تتقدم هذه الجرائم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها ، وحتى الآن فإن الحركة التشريعية ، أو الثقافة الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل ، وهذا الفارق في التقدم أو التطور ينعكس سلباً على فنية إجراء الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة المعلوماتية ، ومن هنا يأتي تقويم تأهيل سلطات الأمن وجهات التحقيق والادعاء والحكم في شأن هذه الجرائم.

ومن المتوقع أن تتضاعف الخسائر في المستقبل القريب بفضل التطور السريع في مجال تقنية المعلومات ، ما لم يتضاعف الاهتمام بالأدلة الرقمية لدى رجال الشرطة والقضاة.

ثم إن التعامل مع مثل هذه المعلومات يحتاج إلى جهود فريق من رجال الشرطة ، والعلوم الجنائية ، والنيابة ، والبرمجة وتحليل النظم ، إذ ليس في مقدور واحد منهم أن يكون ملماً بجميع المهارات اللازمة لكشف خبايا الجرائم ذات العلاقة بالتقنيات العالية ،

فضابط الشرطة قد يكون ملماً بالإجراءات الفنية والقانونية المعتمدة لضبط الجرائم والتحقيق فيها وحماية حقوق الإنسان ، ولكن قد لا يكون ملماً بعلوم الحاسب الآلي والحوسبة والاتصالات ، ومن ثم لن يدرك تماماً ماهية الأدلة الجنائية التي يسعى لها محللو النظم والمبرمجون والمهندسون الذين يفهمون كل شيء عن تقنية المعلومات وشبكات الاتصالات وطريقة عملها ، ولكن قد لا يدركون ما يتصل بمتطلبات الإجراءات القانونية وقواعد البينة وكيفية التعامل معها حتى تبقى الأدلة ذات قيمة برهانية مقبولة أمام المحاكم (1).

إن المتخصصين في علم الحاسوب قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم إلى المحاكمة وفي كثير من الحوادث يظن متخصص الحاسب أن لديه الدليل الحاسم ، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى؛ بينما المحققون ذوو الخلفية القانونية ، كرجال الشرطة مثلاً ، قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم.

ويعتمد النشاط الأمني في هذا المجال على جمع المعلومات السرية عن حركة السوق وتداول الأموال والممتلكات والتغيرات الاجتماعية والسلوكية للموظفين وصغار رجال الأعمال الذين يرتبطون بمؤسسات الجريمة المنظمة. إذ إن جرائم الحاسب الآلي هي من أدوات وأسلحة مرتكبي الجريمة المنظمة الذين يسخرون إمكاناتهم لاستقطاب صغار الموظفين وذوي القدرات الفنية الذين هم على مقربة من أسرار برامج الحاسب الآلي في المؤسسات المالية والشركات التجارية.

1- محمد الأمين البشرى (1423هـ) ، "الأدلة الجنائية الرقمية ودورها في الإثبات" ، المجلة العربية للدراسات الأمنية والتدريب ، س17 ، ع 33 ، ص147-91 , الرياض: جامعة نايف العربية للعلوم الأمنية.

إن تطور ثقافة الحاسب الآلي وسط رجال الأمن وربط تلك الثقافة بالثقافة الأمنية التقليدية يكفل للأجهزة الأمنية نجاحاً في مواكبة ظاهرة جرائم الحاسب الآلي ، فالقدرة على الملاحظة ، وقراءة تصرفات الأشخاص العاملين في مجال الحاسب الآلي ، والمهتمين بالبرامج ، وهواة صناعة الأنظمة وتقليدها هي أولى خطوات السيطرة الأمنية على نشاط مرتكبي مثل هذه الجرائم.

وقد أثبتت الوقائع أنه تم ارتكاب بعض هذه الجرائم على مرأى ومسمع من رجال الأمن ، بل قام بعض رجال الأمن بتقديم يد المساعدة لمرتكبي جرائم الحاسب الآلي دون قصد وعن جهل ، أو على سبيل واجبات المهنة التي يلزمهم بها القانون.

7- **الجرائم المستحدثة :**

أسهم تقدم التقنيات والعلوم الحديثة وتزايد الاعتماد عليها في شئون الحياة في المجتمعات بظهور أنواع وصور مستحدثة من الجرائم التقنية التي تحمل طابع هذه التقنيات وتساير على الدوام تيار تقدمها باعتمادها على التقنية عادة لارتكابها.

وهنا نستعرض الجرائم المستحدثة وماهيتها وعناصرها وطبيعتها ، ونوضحها وذلك على النحو التالي:

1- تعريف الجريمة المستحدثة :

يمكن أن نعتمد في تعريف الجريمة المستحدثة على تعريف الجريمة بصفة عامة ، والتعاريف المختلفة التي صاغها الفقهاء لتعريف الجرائم المنظمة والجرائم الاقتصادية التي تجعلنا نقف على مفهوم الجرائم المستحدثة ، على أنه: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يُرتكب باستخدام أية تكنولوجيا أو تقنية حديثة لتحقيق النتيجة الإجرامية التي يؤثمها المشرع ، أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به ، يتعلق باستخدام أية تكنولوجيا حديثة وتطبيقاتها. أو هي كل فعل أو امتناع عن

فعل من شأنه الاعتداء على الحقوق المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل تقنية أو تكنولوجيا حديثة" [1].

وفي ظل هذا التعريف يكون استخدام المحتالين للحاسب الآلي والإنترنت وبطاقات الائتمان جريمة مستحدثة ، أما استخدام المحتالين لتحقيق جرمهم طريقة المندل أو الزار وغيرهما من الطرق التقليدية ، فإنه لا يعد جريمة مستحدثة في نطاق هذا البحث ، كما تعد سرقة حاسب آلي من منزل أو منشأة أو إحراقه جريمة تقليدية ، أما اختراقه الحاجز الأمني للحاسب الآلي بواسطة استخدام برامج أو تطبيقات التعرف على كلمة السر الخاصة به لاختراقه ، فكلها جرائم تدخل في نطاق الجرائم المستحدثة في هذا البحث.

وعليه ، فإن تنفيذ الجريمة المستحدثة يجب أن يتوافر فيه مجرم واحد على الأقل قادر على توظيف التكنولوجيا في ارتكاب جريمته ، أو يشارك آخرين في ارتكابها ، ويكون على درجة عالية من الذكاء والمهارة التي يتطلبها استخدام التقنية العلمية والتكنولوجيا.

كما يتطلب تنفيذ الجرائم المستحدثة ضرورة أن يتوافر في المجرم الثقافة العلمية والتفكير الابتكاري حتى يستطيع أن يوظف تقنية حديثة في ارتكاب جريمة تقليدية ، هذا بالإضافة إلى أن معظم مرتكبي الجرائم المستحدثة يكونون من غير أصحاب السوابق ، كما تكون نسبة غير قليلة منهم من الموظفين الحاليين أو السابقين للأجهزة أو المؤسسات التي وقع عليها الجرم ، ويشكل الذكور نسبة كبيرة من الجناة في مثل هذه الجرائم.

كما أن المجني عليه في الجرائم التقليدية عادة ما يكون شخصاً محدداً أو مجموعة محددة من الأشخاص ، أما في الجرائم المستحدثة فعادة ما يقع الضرر على مصلحة المجتمع كله ، فمثلاً جريمة غسل الأموال القذرة يقع ضررها على الاقتصاد القومي.

1- محمد شفيق (1995م) ، الجريمة والمجتمع ، الإسكندرية: المكتب الجامعي الحديث ، ص 31.

والدافع إلى الجريمة قد يختلف في الجرائم المستحدثة عنه في الجرائم التقليدية ، ففي الأولى يكـون الدافع نابعاً من التشويق والتجربة والزهو ومحاولة إثبات التفوق على الآلة ، والرغبة في هزيمة أنظمة التأمين الموضوعة ، وهذا كله يشكل جانباً كبيراً مـن البواعـث والدوافع لارتكاب بعض الجرائم المستحدثة وخاصة الجرائم المعلوماتية [1].

2- طبيعة الجرائم المستحدثة :

تتميز الجرائم المستحدثة بطابع خاص يميّزها عن الجرائم التقليدية وذلك للأسـباب الآتية:

1- عدم ترك هذه الجرائم لأي أثر خارجي بصورة مرتبة.
2- هذه الجرائم لا عنف فيها ، ولا جثث لقتلى ، ولا آثار لدماء.
3- يتم اكتشاف معظمها إن لم يكن جميعها بالمصادفة البحتة ، والدليل على ذلك أنـه لم يكتشف (1%) فقط منها ، وإن (15%) منها تم الإبلاغ عنهـا ، وأن خمـس النسبة الأخيرة هي التي تصدر فيها أحكام بإدانة مرتكبيها.
4- ترتكب في الخفاء في أغلب الأحوال ولا يوجد لها أثر كتابي.
5- قدرة الجاني على تدمير ما قد يُعد دليلاً لإدانته في أقل من ثانية واحدة.
6- إمكانية ارتكاب هذا النوع من الجرائم خلال مسافات بعدية قد تصـل إلـى دول وقارات.

3- أنواع الجرائم الالكترونية :

هناك أنواع عديدة من الجرائم التي تلتصق بشبكة الإنترنت حتى اشـتهرت بـــ (جرائم الإنترنت) ومن أبرزها:

1- عمر حسن عدس (1995م) ، جرائم الحاسب الآلي وأشكالها وأساليب مواجهتها ، "بحث مقدم لمؤتمر قادة الشرطة والأمن العرب ، 16ـــ1995/10/18م) ، ص 109.

- **الاختراق (Hacking / Gracing):**

تقوم فكرة الاختراق على مبدأ بسيط وهو قدرة الهكر على كسر الحواجز البرمجية الخاصة بمنع الاتصال بجهاز الحاسوب من خلال الشبكة إلا للأشخاص المصرح لهم فقط حيث يتمكن من الاطلاع على البيانات الموجودة داخل هذه الحواسيب كلياً أو جزئياً وقد يتمكن من سرقتها أو إتلافها أو تعديلها إذا أراد ذلك [1] [2].

وقد تعرض موقع الأمم المتحدة مؤخراً للاختراق من قبل قراصنة الإنترنت (الهاكرز) ، حيث تم إغلاق بعض الأقسام ، ومن جهة أخرى تم تشويه الصفحة الخاصة بالأمين العام (بان كي مون) وظهرت شعارات تتهم الولايات المتحدة وإسرائيل بقتل الأطفال والناس العاديين ، مع المطالبة بنشر السلام وإيقاف الحروب ، المجموعة المخترقة مكونة من ثلاثة أشخاص إذ سبق وهاجمت العديد من المواقع على الانترنت وقامت الأمم المتحدة بإصلاح صفحة الأمين العام في وقت لاحق واضطرت إلى إغلاق بعض الصفحات لحين إصلاحها.

وطريقة الاختراق وفقاً لموقع (Hackedemix.net) تمت بما يسمى (SQL Injection) وتعد نقطة ضعف مشهورة جداً ومن السهل تفاديها ؛ لذا ينبغي عدم وجودها في موقع بارز مثل موقع الأمم المتحدة ، وتم استخدام هذه الطريقة في إغلاق وتشويه العديد من المواقع الحكومية والتجارية حول العالم ، ولعل أقربها تعرض موقع شركة مايكروسوفت بريطانيا لهجوم (SQL Injection) اختراق جرائم [3].

1- Denning, D.& Baugh, E.(1999).Hiding crime in Cyberspace. [online]Available.

2- محمد السرحاني (2004م) ، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت ، الرياض: جامعة نايف العربية للعلوم الأمنية.

3- جريدة الرياض ، عدد 2007/8/14م.

- **تدمير البيانات الحاسوبية (Data Sabotage) :**

يعرف تدمير بيانات الحاسوب بأنه التدخل في العمليات الحاسوبية بالتسبب في ضرر متعمد لدائرة الحوسبة أو للأجهزة [1].

ويرى ستيفنسون أن الهكر الهواة الذين يستخدم لوصفهم مصطلح (Crackers) غالباً ما يخترقون الحواسيب بدافع الفضول وحب التعلم ، ولذلك فإنهم نادراً ما يقومون بتدمير البيانات أو الاحتيال أو غير ذلك من الأفعال التي حصر القيام بها في المجرمين المحترفين [2].

- **استخدام الشفرة الخبيثة :**

الشفرة الخبيثة (Malicious) ، هي برمجيات صممت لتنتقل من حاسوب إلى آخر ومن شبكة إلى أخرى بهدف إجراء تعديلات في أنظمة الحاسوب عمدا وبدون موافقة مالكي أو مشغلي هذه الأنظمة ، ويوجد من هذه البرمجيات الكثير حالياً ، كما أنه يصدر منها العديد يومياً في أنحاء متفرقة من العالم [3].

- **الاحتيال (Cyber Fraud) :**

الاحتيال مستخدم بشكل كبير وبأشكال متعددة منها الترويج لخدمات وسلع على الإنترنت ، وبعد أن يقوم المشتري بإرسال المال إلى البائع لا تصله البضاعة المشتراه ، أو يصله شيء أقل بكثير مما كان يروج له على الإنترنت.

1- Furnell, Steven (2002) .Cybercrime: Vandalizing the information society Boston : Addison-Wesley.
2- Stephenson, Peter (2000). Investigating Computer-Related Crime. Boca Raton, Florida: CRC Press.
3- Grimes, Roger (2001). Malicious Mobile Code. Sebastopol, California: O'Reilly & Associates.

ومن أشكال الاحتيال أيضاً ، استغلال البيانات الحاسوبية وذلك بتعديلها بما يقدم فائدة مادية للشخص الذي يقوم بالتعديل على حساب خسارة يتسبب فيها للمالك ، وبعض هذه الأفعال قد تصدر من موظفين بحق أصحاب أعمالهم ، كالتلاعب في السجلات الضريبية لصالح بعض أصحاب الأموال [1].

- **جرائم النصب عبر الإنترنت :**

تعد جرائم النصب التي ترتكب عن طريق الحاسبات أخطر أنواع جرائم النصب التي يخشاها المشرعون ورجال القانون ، فتلك الجرائم لا يمكن أن تخضع لمعايير ومقاييس معينة ، كما أنه يصعب التعرف عليها وفهم أبعادها وحيثياتها ، ومن أخطر جرائم النصب التي ترتكب على الحاسبات هي تلك الجرائم التي يخطئ فيها الموظفون ويقومون بتدوين بيانات وأرقام أكبر من الأرقام الحقيقية ، ما يتسبب في خسائر فادحة ، والحاسب من الناحية الشائعة والقانونية هو الوسيلة التي ترتكب الجريمة من خلالها أو توفر بيئة الجريمة.

وخلال الفترة ما بين عامي (1984–1987م) تم اكتشاف 168جريمة نصب عن طريق الحاسب الآلي في انجلترا وويلز ، وقدرت الخسائر الناجمة عن تلك الجرائم بنحو(2,5) مليون جنيه استرليني ، كما أكده ليولد ، وتؤكد مصادر أخرى أن الخسائر الناجمة عن هذه الجرائم تتراوح بين (300) مليون جنيه استرليني و(2) مليار جنيه إسترليني ، ويرى رجال الشرطة أن كشف جريمة النصب يعد أمراً بالغ الصعوبة ، ويذكر ليولد إحدى الجرائم حينما قام أحد موظفي البنوك بنقل (45.000) جنيه من الحساب الثابت لشخص ليوضع في حسابه اعتماداً على نغمة الصوت (شفرة الصوت) بمجرد أن غادر هذا الشخص البنك ومن أجل ألا يكتشف أمره قام ببرمجة الحاسب لإبقاء كل المعاملات التجارية التي تمت عليه.

1- Denning, D.& Baugh, E.(1999).Hiding crime in Cyberspace. [online]Available.

وهناك جرائم نصب أخرى يستخدم فيها الحاسب ، فقد يقوم موظفون أو آخرون باستخدام الحاسب بشكل سيء لأغراض دنيئة.

ومن المقلق بالنسبة لهذه الهيئات الطريقة التي يستخدم بها الأشخاص الحاسب في الوصول لأهداف دنيئة فقد يستخدم هؤلاء الأشخاص البيانات في أغراض غير قانونية ، فجرائم النصب التي ترتكب خلال الحاسب أو عبر الحاسب هي جرائم خطيرة رغم اختلافها عن جرائم النصب التقليدية ، إلا أن محض خطورتها هو كونها تلاعباً بالبيانات لا بالسلع.

- **مضايقة الغير (Harassment) :**

ويمكن أن يتم ذلك في بيئة الحاسوب والإنترنت من خلال البريد الإلكتروني ، حين يتلقى شخص ما أي نوع من رسائل التهديد سواء بالإيذاء أو الموت من خلال صندوقه البريدي [1].

ومن أشكال الأنشطة المشبوهة على الإنترنت والتي ينجم عنها مضايقة وإزعاج الغير ، والملاحقة ، والمطاردة (Stalking) التي يقوم بها أحد الأشخاص بملاحقة الغير على الإنترنت من خلال المنتديات وغرف الدردشة والبريد الإلكتروني ، والتحرش بهم وربما نشر بعض المعلومات عنهم بقصد المضايقة أو الترويع في بعض الأحيان ، حيث تكون الضحية في غالب الأحيان من النساء.

- **غسل الأموال (Cyber-Laundering) :**

تؤدي التجارة الإلكترونية دوراً مهماً في عقد الصفقات عبر الإنترنت كصفقات السيارات والعقارات أو المعادن الثمينة ، كما يمكن أن تسهم الأنظمة الحاسوبية التي تعمل في البنوك في مساعدة المجرمين على إيداع أموالهم ذات المصدر المشبوه ، ومن ثم إعادة

1- Denning, D.& Baugh, E.(1999).Hiding crime in Cyberspace. [online]Available.

سحبها في الخارج بعملات صعبة كالدولار مثلاً ، ويكون مصدرها مشروعاً في الظاهر خاصة ما يعرف (Cyber Banking) أي البنوك عبر الإنترنت ، حيث تتم جميع التعاملات المصرفية والحوالات بأية مبالغ من خلال الاتصال بالمواقع الافتراضية لهذه البنوك عبر الإنترنت في سرية وخصوصية ، وهو ما يتيح لغاسلي الأموال بيئة مناسبة لإجراء تحويلاتهم المشبوهة.

- **انتحال شخصية المواقع :**

يعد أسلوب انتحال شخصية المواقع على شبكة الإنترنت (Web Spoofing) من الأساليب الحديثة نسبياً في عالم جرائم نظام المعلومات ، لكنه أشد خطورة وأكثر صعوبة في اكتشافه من أسلوب إخفاء الشخصية (IP Spoofing) ، ومن المتوقع أن يكثر استخدام هذا الأسلوب في جرائم نظم المعلومات في المستقبل ، ولتنفيذ هذه الجريمة يستفيد المجرم من حقيقة أن أي كمبيوتر على الإنترنت يمكن أن يقحم نفسه في موقع بيني أي بين البرنامج المستعرض (Browser) للحاسب الخاص بأحد مستخدمي الإنترنت وبين الموقع (Web) ، ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي ، ويستطيع مراقبة أي معلومات متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه ، كما يستطيع سرقة هذه المعلومات أو تغييرها ، وتمتد هذه الثغرة إلى برامج استعراض المواقع الحالية الشهيرة [1].

8- تجارب وتطبيقات :

1-آفاق التقنية المعلوماتية بالمملكة العربية السعودية :

بادرت المملكة العربية السعودية إلى اقتناء هذه التقنية والاستفادة منها ، ونظراً إلى اتساع رقعة المملكة جغرافيا وزيادة عدد سكانها بصورة متسارعة إضافة إلى أنها تضم المشاعر المقدسة التي يزورها الملايين سنوياً؛ فإن حاجة المملكة إلى بنية اتصالات

1- حسن داود (2000م) ، جرائم نظم المعلومات ، الرياض: جامعة نايف العربية للعلوم الأمنية.

ومعلومات أصبحت قوية متزايدة ، وتتكون بنية الاتصالات بالمملكة من خطــوط (TTM) الوطنية الفائقة السرعة ، إضافة إلى خطوط الهاتف الرقمية والتقليدية والاتصالات الفضائية بأنواعها.

أما أجهزة الحاسب الآلي فإن المملكة تحتوي على ما لا يقل عن (500,000) جهاز حاسب آلي تنمو بنسبة (122%) سنوياً ، إضافة إلى هذا يمثــل الحاســب الآلــي ونظــم المعلومات العمود الفقري لمعظم المؤسسات الحكومية والأهلية ويتم الاتصــال بالإنترنــت الدولية في السعودية عن طريق مدينة الملك عبد العزيز للعلوم والتقنية وهي الجهة المسئولة عن توفير الخدمة (هناك بعض التغيّرات بعد إنشاء وزارة الاتصالات وتقنيــة المعلومــات وزيادة دور هيئة الاتصالات وتقنية المعلومات وحجب المواقع السيئة).

- **ملامح الجريمة والتعاملات الالكترونية في المملكة العربية السعودية :**

تشير إحدى الدراسات إلى أن المملكة تحتل الترتيب الخامس على المستوى العالمي من حيث معدل نمو عدد أجهزة الحاسب الآلي المستخدمة ، وهي أكبر أسواق منطقة الشرق الأوسط في أعداد الأجهزة المبيعة ويتجاوز عدد مشتركي الإنترنت 600 ألف مشترك ، كما تم تسجيل أكثر من (4,500) اسم نطاق بالمملكة وتقدر نسبة النمو فــي قطــاع الإنترنــت بالسوق السعودية أكثر من (275%) [1].

ويلاحظ المتابع لواقع تقنية المعلومات بالمملكة ندرة القضايا الأمنيــة والقضــائية المنشورة والموثقة المتعلقة بها ؛ إلا أن هذا الواقع لا يعكس حقيقة الأمور في ظل غيــاب الإحصاءات الرسمية لتلك القضايا وعدم وعــي المجتمــع المحلــي بمخاطرهــا وجهــات الاختصاص التي يمكن الرجوع إليها عند الحاجة ، يضاف إلى ذلك حداثة الثــورة التقنيــة بالمملكة – نسبياً ، وخصوصاً تقنية المعلومات والدخول في المواقع الإلكترونية.

1- سليمان العنزي (2003م). وسائل التحقيق في جرائم نظم المعلومات. "رسالة ماجستير غير منشــورة" ، الرياض: أكاديمية نايف العربية للعلوم الأمنية, الرياض.

- **البعد الوقائي للجرائم الإلكترونية في المملكة العربية السعودية :**

يعني البعد الوقائي بوضع الحواجز التي تمنع وقوع الجريمة سواء بمنع الوصـــول إلى أماكنها (كقيام مدينة الملك عبد العزيز للعلوم التقنية بحجــب المواقــع الإجراميـــة) أو بتقليص منافذها (كقيام إدارات الحاسب الآلي بنزع سواقة الأقراص المرنة لمنـــع دخـــول الفيروسات وأحصنة طروادة عبر الملفات المنسوخة مـــن تلـــك الأقــراص) ، أو تركيـــب البرامج المكافحة للفيروسات ولجدار الحماية ، وهذا البعد المهم يعمل بالتوازي مع مسارات الجريمة المذكورة للحيلولة دون حصول الجريمة ، وينبغي أن تسعى كل جهة من جهـــات النموذج إلى توفير وسائل الوقاية من الجريمة المعلوماتية.

ومع أهمية تلك الاحتياطات الوقائية فإن الضحية من مستخدمي تقنية المعلومات يظل غالباً المسؤول الأول عن حماية نفسه [1].

- **نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية :**

أقر مجلس الوزراء بالمملكة العربية السعودية في جلسته بتـــاريخ 1432/7/3هــــ نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية ، حيث أتى صدور هذين النظامين للحد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات ، وبما يـــؤدي إلـــى تحقيق الأمن المعلوماتي وزيادة استخدامات الحاسب وشبكاته ، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات والشبكات ، وحماية المصـــلحة العامـــة والأخـــلاق والآداب العامة تعزيزاً لاستخدام التعاملات الإلكترونية على الصعيدين المحلي والدولي ، وللاستفادة منها في جميع المجالات كالتجارة ، والطب ، والتعليم ، والحكومة الإلكترونيـــة ، والـــدفع الإلكتروني ، والى غير ذلك من التطبيقات والممارسات ذات الأبعاد التطويرية والتنموية ،

1- محمد القاسم ورشيد الزهراني (1427هــ) ، نموذج مقترح للتعامل مع جـــرائم المعلوماتيـــة بالمملكـــة العربية السعودية. مجلة البحوث الأمنية ، ع22 ربيع الأخر 1427هــ.

وإزالة أي عائق أمام استخدام التعاملات والتوقيعات الإلكترونية والحد من حالات إساءة الاستخدام وفرص الاحتيال في التعاملات والتوقيعات الإلكترونية ، كالتزوير والاختلاس.

ولإلقاء الضوء على هذا النظام أورد هنا بعض مواده الداعمة للوقاية والمكافحة ، فقد جاء في المادة الحادية والثلاثين (الفقرة الثانية) ما يلي :

- المساعدة على تحقيق الأمن المعلوماتي ، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية حماية للمصلحة العامة ، وحماية الاقتصاد الوطني.
- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا. الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع ، أو إتلافه أو تعديله أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا ، أو ما في حكمها ، والتشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة.

وفي المادة الرابعة ، جاء ما يلي:

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال ، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات ، أو أي من أعضائها أو ترويج أفكارها أو تمويلها ، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات ، أو أداة تستخدم في الأعمال الإرهابية.

2- الدخول غير المشروع إلى موقع إلكتروني ، أو نظام معلوماتي مباشـرة أو عـن طريق الشبكة المعلوماتية ، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني [1].

2- أمريكا :

التي تزداد فيها ظاهرة الإجرام عبر الإنترنت وتتضاعف فيها الخسائر الناتجة عـن تلك الظاهرة والتي تلحق بالقطاعات العامة أو الخاصة ، فقد تم وضع عدة أقسام ووحـدات للشرطة لمواجهة هذا الإجرام والحد من خسائره ومنها:

- قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية الذي تم إنشـاؤه سـنة 1991م والذي يختص بالكشف عن جرائم الحاسب الآلي وحقوق الملكيـة الفكريـة وعـن ملاحقة مرتكبيها.
- معهد أمن الحواسيب.
- وحدة جرائم الإنترنت ، وهي وحدة تختص بالتحقيق في جـرائم حقـوق الملكيـة الفكرية في الجرائم المرتبطة بالتقنية العالية ويترأسها مدير مساعد لمكتب التحقيقات الفيدرالي.
- مكتب رئيس التكنولوجيا: وهو مكتب مفوض مباشرة من مكتب مـدير التحقيقـات الفيدرالية الأمريكي لتسيير مختلف المشروعات التكنولوجيـة وملاحقـة مرتكبـي الجرائم الواقعة في ذلك المجال.
- كما تم إنشاء المركز الوطني لحماية البنية التحتيـة التـابع للمباحـث الفيدراليـة الأمريكية في مطلع العام 1998م ، الذي يتقاسم مهامه مع وزارة الـدفاع ، وهـو يتكون من فريق سري يصل عدد أعضائه إلى 125 عضواً.

وتجدر الإشارة هنا إلى أن نشأة هذا الفريق تعود إلى تقرير حكومي ، جمعية العمل حول جرائم الانترنت ، والمقدم إلى الرئيس الأمريكي السابق "بيل كلينتون" والذي حـددت

1- جريدة الرياض ، عدد 2007/8/14م.

من خلاله البنى التحتية التي تعد هدفاً للهجمات والاعتداءات عبر الانترنت ، والمتمثلة في: الاتصالات ، والكهرباء ، والغاز ، والبترول ، ووسائل النقل.

3- بريطانيا :

وفي إطار مكافحتها لجرائم الإنترنت فقد تمت زيادة عدد أفراد الشرطة والدرك المتخصصين في البحث والتحقيق في هذا النوع من الجرائم ليصل عددهم سنة 2008م إلى 600 شرطي ودركي. إلى جانب حسن تنظيم أشغالهم وتقوية قدراتهم القانونية في التحقيق في مراقبة كافة أشكال العدوان الإلكتروني التي يمكن أن ترتكب أو تكون تلك الشبكة محلاً لها كالإرهاب والقرصنة المعلوماتية والعنصرية والسامية وإرهاب الأجانب (XENAPHOBIE).

4- هونج كونج :

تأسست "قوة مكافحة قرصنة الإنترنت" في ديسمبر 1999م ، واستطاعت القبض على 12 شخصاً في خمس قضايا في ظرف ستة أشهر من تأسيسها.

5- الصين :

فقد تأسست "القوة المضادة للقرصنة" في عام 2000م وتتخذ من المعهد العالي للطاقة الفيزيائية مقراً لها ، وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الانترنت ، إذ تلزم مستخدم شبكة الانترنت بتسجيل نفسه لدى مكاتب الشرطة.

5- فيتنام :

كما تم تشكيل وحدة خاصة من الشرطة في **فيتنام** للتحقيق في جرائم الانترنت والحد من توزيع المنشورات المحظورة من خلالها [1].

1- نبيلة هروال (2006م) ، الجوانب الإجرائية لجرائم الانترنت ، بيروت: دار الفكر الجامعي.

المبحث الثاني
التحقيق في الجرائم الإلكترونية

1- شرطة الإنترنت (Cyber Police) :

هي شرطة متخصصة لمواجهة هذا الإجرام المستحدث وتقوم بإجراءات وضمانات للمحافظة على أموال الغير ، وهناك بعض الدول عنيت بتزويد محققي الشـرطة بمعـارف ومهارات خاصة حول البرمجة. ويراعى في تكوينها أن تكون متخصصة ومستعدة دائمـاً للتعامل مع هذه النوعية من الجرائم ، وذلك عن طريق تدريبها وتكوينها في أمـور تقنيـة الحوسبة والانترنت ، وفي كيفية التعامل مع هذا العالم الافتراضي ،غير أن هنـاك بعـض الإشكاليات ، منها: أن انتشار الانترنت وإمكانية ارتكاب سلوك سلبي عبرهـا ، يسـتدعي إعادة النظر في تفسير المشروعية في بعض الأعمال والمهام ، كما هو الشأن في التخفـي عبر الاتصالات وإمكانية انتحاله أسماء وهمية ودخوله في حلقات النقاش وممارسته للتراسل الإلكتروني بقصد الكشف عن الجرائم.

وفي حالة القيام بالإجراءات التي تمس وتقيّد حرية المتهم أو المشتبه فيه ، كالتفتيش والضبط والقبض ، في الحالات الاستثنائية ، أن يستصدر إذناً من السلطات المختصة للقيام بتلك الإجراءات.

أ- التحقيق في الجرائم الإلكترونية :

إن المواصفات والخصائص المختلفة لجرائم الحاسب الآلي أوجدت في الكثير مـن المشاكل العملية في التحقيق والإثبات ، وتبرز في نوع الدليل المعتمد للإثبات ، وصـعوبة كشفه وضبطه ، واحتياجه إلى أهل الخبرة والفن.

وإن التعرض إلى المبادئ الأساسية في الجرائم المعلوماتية يقتضي أن تعرض إلـى العناصر الأساسية للتحقيق ، وضمانات المتهم في مرحلة التحقيق الجنائي ، وذلـك علـى النحو التالي:

أولاً – العناصر الأساسية للتحقيق في الجرائم المعلوماتية :

يجب على المحقق أن يستظهر الركن المادي ، والركن المعنوي للجريمة محل التحقيق ، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية بالإضافة إلى علانية التحقيق ، وهو ما سنعرض له على النحو التالي:

العنصر الأول – إظهار الركن المادي للجرائم المعلوماتية :

إن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت ، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته ، فمثلاً يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة ، فيقوم بتحميل الكمبيوتر ببرامج اختراق ، أو أن يقوم بإعداد هذه البرامج بنفسه ، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف (Hosting Server) ، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية ، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية ، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء ، فشراء برامج اختراق ، وبرامج فيروسات ، ومعدات لفك الشفرات وكلمات المرور ، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

العنصر الثاني – إظهار الركن المعنوي للجرائم المعلوماتية :

الركن المعنوي هو الحالة النفسية للجاني ، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني ، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم ، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية

في القانون الفيدرالي الأمريكي ، وأحياناً أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.

العنصر الثالث – تحديد وقت ومكان ارتكاب الجريمة المعلوماتية :

تثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة ، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية ، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم (Server) أحد البنوك في الإمارات ، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة ، هل هو توقيت بلد المجرم أو توقيت بلد البنك المسروق أو توقيت الجهاز الخادم في الصين ، ومن ثم يثير مشكلة أخرى وهي مكان ارتكاب الجريمة المعلوماتية ، ويثير أيضاً إشكاليات القانون الواجب التطبيق في هذا الشأن ، حيث إن هناك بعداً دولياً في هذا المجال ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود [1].

العنصر الرابع – علانية التحقيق :

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة ، ولهذا قيل إن العلانية في مرحلة المحاكمة لا يقصر فيها الأمر على وضع الاطمئنان في قلب المتهم ، بل إن فيها بذاتها حماية لأحكام القاضي من أن تكون محلاً للشك أو الخضوع تحت التأثير ، كما أن فيها طمأنة للجمهور على أن الإجراءات تسير في طريق طبيعية.

ولا شك فإن العلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة به ، وهي تختلف في التحقيق الابتدائي عنها في مرحلة المحاكمة ، ففي الابتدائي تعد العلانية نسبية أي مقصورة على الخصوم في الدعوى الجنائية ، والعلانية في التحقيق النهائي – أو مرحلة المحاكمة – هي علانية مطلقة ، بمعنى أنه يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة.

1- خالد ممدوح إبراهيم (2009م) ، الجرائم المعلوماتية ، دار الفكر الجامعي.

على أن المشرع يجيز في المرحلتين – التحقيق الابتدائي والتحقيق النهائي – مباشرة الإجراءات في غير علانية ، فيصدر القرار بجعله سرياً ، وهذا استثناء يأتي لسيادة كل دولة على إقليمها ويخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية.

ويلاحظ في هذا المجال تصادم التفتيش مع الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية ، وذلك لأن هذا التفتيش يتم – غالباً – على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات ، الأمر الذي قد يتجاوز النظام المعلوماتي المشتبه به إلى أنظمة أخرى مرتبطة ، نظراً لشيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى الدول. ولا شك في أن امتداد التفتيش إلى نظم غير النظم محل الاشتباه قد يمس – في الصميم – حقوق الخصوصية المعلوماتية لأصحاب النظم المعلوماتية التي يمتد إليها التفتيش.

ب- إجراءات التحقيق في الجرائم المعلوماتية :

تنقسم إجراءات التحقيق إلى قسمين: قسم يهدف إلى التنقيب عن الحقيقة سواء ما يتعلق بثبوت التهمة أو عدم ثبوتها أم ما يتعلق بنسبتها إلى المتهم ، وذلك بالبحث في الأدلة وتمحيصها وهو ما يطلق عليه "إجراءات التحقيق" في معناها الدقيق ، ويطلق عليها فقهيًّا في مصر تعبير إجراءات جمع الأدلة.

أما القسم الثاني فلا يشمل إجراءات التحقيق بالمعنى الدقيق ، لأنها لا تستهدف بحثاً عن أدلة ، وإنما هي أوامر تحقيق تستهدف تأمين الأدلة من أسباب التأثير أو العبث ويطلق عليها الفقه " الإجراءات الاحتياطية ضد المتهم" ، وهي الأمر بحضور متهم والأمر بالقبض عليه وإحضاره والأمر بحبسه احتياطياً (ولكون هذه الإجراءات خارج نطاق بحثنا فلا حاجة للاستضافة المفصلة فيه).

أما إجراءات التحقيق محل الدراسة ، فنقصد بها مجموعة الإجراءات التي تهدف إلى التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه ، وأهم هذه الإجراءات هي التفتيش ، والانتقال ، والمعاينة ، وندب الخبراء ، وسماع الشهود ، والاستجواب.

وتهدف إجراءات التحقيق في الجرائم المعلوماتية إلى جمع وفحص الأدلة القائمة على وقوع الجريمة ونسبتها إلى فاعلها ، وهي لم ترد في القانون على سبيل الحصر ، بل يمكن مباشرة أي إجراء يفيد في كشف الحقيقة ما دام أن المحقق تقيّد في مباشرته بحدود المشروعية.

والمشرع المصري لم يلزم المحقق باتباع هذه الإجراءات وحدها دون غيرها من أجل التنقيب عن الحقيقة ، إذ يجوز للمحقق أن يلجأ إلى غير هذه الإجراءات ما دام رأى أن فيها فائدة في كشف الحقيقة ، ولم يكن في مباشرتها مساس بحرية المواطن أو بحرمة مسكنه ، إلا أن القانون ألزم المحقق بإجراء واحد هو استجواب المتهم.

ومن جهة أخرى لم يلزم المشرع المصري المحقق الجنائي باتباع ترتيب معين ضد مباشرته لإجراءات التحقيق ، بل ترك له وحده سلطة تقدير بأي هذه الإجراءات يبدأ على ما يراه ضرورياً وفقاً لظروف الحال.

ج – إجراءات التحقيق في الجرائم الإلكترونية :

وهناك تشابه بين التحقيق في جرائم الحاسوب والإنترنت وبين التحقيق في الجرائم الأخرى ، فهي جميعا تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع وتحليل الأدلة ، كما أنها تشترك في

كونها تسعى إلى الإجابة عن الأسئلة الستة المشهورة لدى المحققين ، ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا ؟ (1).

إلا أن جرائم الحاسوب والإنترنت تتطلب الاطلاع على كمية ضخمة من السجلات بأجهزة الحاسوب (Computer Manuals) وملفات تسجيل العمليات الحاسوبية (Log Files) وغيرها ، كما أن التحقيق يجري هنا في بيئة رقمية. وفي مرحلة جمع الاستدلالات يلتزم بتحرير محضر يثبت فيه كل ما اتخذه من إجراءات للكشف عن الجريمة من انتقال إلى مسرح الجريمة ، ومعاينته وضبطه وسماع الشهود .. والحال لا يختلف في بيئة الإنترنت التي وقعت فيها الجريمة ، وتحرير ذلك المحضر عبر الانترنت ، وذلك وفق الخطوات التالية:

أولاً: تلقي جهة التحقيق معلومات أمنية تشير إلى ممارسة شخص معروف أو غير معروف لأنشطة تندرج تحت تعريف جريمة الحاسب الآلي وذلك في مكان معروف وعلى أجهزة محددة ، ووفق لغات برمجية معلومة.

ثانياً: ضبط شخص وبحيازته أموال مشبوهة أو بطاقات ائتمان مزورة أو بطاقات تعريف مشبوهة.

ثالثاً: بناء على بلاغ يصل إلى علم جهة التحقيق من متضرر يفيد وقوع تلاعب أو ممارسات خاطئة في حقه أو حق آخرين ، سواء كان ذلك في شكل من أشكال عجز مالي في حسابات مؤسسة مالية أو ضياع حقوق أو تغيّرات في الودائع.

رابعاً: توفر معلومات عن نشر فيروسات تخريبية عبر شبكات إنترنت.

خامساً: توفر معلومات عن وقوع عمليات اعتراض أو قرصنة فضائية للمعلومات.

1- Stephenson, Peter(2000). Investigating Computer-Related Crime. Boca Raton, Florida: CRC Press.

د- صعوبات جمع الأدلة في الجرائم الإلكترونية :

تتم هذه الجرائم في الغالب ضمن بيئة افتراضية غير مادية ، على شكل نبضات إلكترونية غير مرئية ، ومن ثم لا تترك أي دلائل مادية ، ولذا تبرز مشاكل كثيرة في جمع أدلة هذه الجرائم ومن أهمها:

- **محو الدليل أو تدميره :** لما كانت الجريمة المرتكبة على الحاسب الآلي (إتلاف بيانات) أو بواسطته (سب ، قدح) تتم بإشارات وأوامر معنوية تعطى من الجاني للحاسب الآلي المنفذ ، فإن مسالة التخلص من تلك الأوامر أمر بغاية البساطة ، خصوصاً عندما تكون الجريمة واقعة بسلوك جرمي واحد يمثل الضغط على أحد أزرار لوحة التحكم في الحاسب الآلي ذاته ، وهي مشكلة تقود إلى أخرى أعقد وأخطر ، وهي صعوبة تحديد الفاعل وكشفه ما يجعل المصادفة المحضة الوسيلة الوحيدة لذلك.
- **صعوبة الوصول إلى الدليل :** يعمد الجاني هنا إلى إعاقة وصول جهات التحقيق إلى الحيز المعنوي المشتمل على الدليل بوضع منظومات حماية تمنع أي دخول غير مشروع للأنظمة والبرمجيات والملفات ، ومن ثم صعوبة نسخها ، يستخدم الجاني لذلك كلمات سر معينة أو وضع تعليمات تعمل على إتلاف الدليل عند أي محاولة للدخول غير المصرح به إليه ، مثل هذه الأوامر المتطورة جداً ذات خطورة كبيرة ممكن أن تضيع فرصة الاتهام على النيابة العامة ، والفرصة الوحيدة للنيابة العامة في حفظ وحماية الدليل تكمن في اكتشاف المعادلة وتحليلها وفك رموزها قبل عمل أي شيء بالحاسب الآلي ، وهو الأمر الذي يحتاج إلى خبرة وفن واختصاص.
- **ضخامة فحص آلاف الصفحات لجمع الأدلة :** في كثير من الأحيان تجد جهات التحقيق أنفسها مجبرة على تفتيش نظام الحاسب الآلي برمته بحثاً عن الدليل ، وهو الأمر الذي يحتاج إلى فحص آلاف الصفحات خصوصاً عندما لا تثبت تلك الصفحات شيئاً ، بالإضافة إلى الحالات التي يكون فيها الحاسب الآلي متصلاً بشبكة الاتصالات العالمية فتزداد الصعوبة وترتفع التكاليف. والأمر هنا يتطلب

خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجود الدليل وأقصر وأيسر السبل لضبطه.

- **قلة الخبرة وضعف الثقافة بتقنية المعلومات** : من البديهي ونحن نتحدث عن جرائم تقع في بيئة الحاسب الآلي ، أن تكون تلك الجرائم معتمدة بشكل أساس على تقنية المعلومات ووسائل التقنية ، الأمر الذي يظهر تطوراً في وسائل ارتكاب الجريمة وفي نوع الدليل وطبيعته ، وفي طريقة كشفه وضبطه. وهناك صعوبة أخرى في جمع الأدلة الرقمية من جداول الحالة التشغيلية في البروتوكولات والاتصالات ، وتتمثل هذه الصعوبة في أن هذه الجداول تكون متاحة لفترات قصيرة ولا يمكن التغلب على هذه الصعوبة بالتحفظ الجنائي على أجهزة الهارد وير (Hard Ware) لحين الفحص ، لأن هذه الجداول تزال تلقائياً بمجرد غلق أو انقطاع التيار الكهربائي عن تلك الأجهزة ، لذلك فمن المستحسن أن يتم استخدام أسلوب (Cut and Past) أي القص واللصق إلى ملف جديد خاص بجمع الأدلة وقبل غلق الأجهزة.

ورغم أن أسلوب القطع واللصق أسلوب ناجح لجمع الأدلة ، إلا أن المشكلات القانونية المترتبة على قانونية هذا الأسلوب قد تثير بعض الشك في مدى سلامة جمع المعلومات وحجيتها أمام أجهزة العدالة الجنائية.

هـ- المهارات المطلوبة لرجال التحقيق في الجرائم الإلكترونية :

هناك جملة من المهارات التي يلزم توافرها في رجال التحقيق في الجرائم الإلكترونية من أهمها :

- تكريس العمل العلمي والفني لإعداد نخب متميزة من المحققين يتمتعون بمهارات متقدمة تساير ما تتطلبه طبيعة هذا التحقيق في هذه الأنواع من الجرائم.
- الارتقاء بهذا الحقل حتى يشعر المحقق على الأقل بالندبة أمام المتهم الإلكتروني.
- إنشاء المراكز والوحدات المتخصصة بالتحقيق في هذه الجرائم وتوفير الإمكانات المالية والفنية التي تعد جزءاً لا يتجزأ من المهارات المنشودة في هذه الميادين.

- انتقاء العناصر المتفوقة فنيًّا وعلميًّا وموهبةً لهذا الحقل والعناية الخاصة برعايتها نفسيًّا وصحيًّا واجتماعيًّا ، لأن طبيعة هذه المهام التي تؤدى في مسرح جريمة تنبض بعوامل نفسية وذهنية.
- اكتساب مهارات خاصة تسمح باستيعاب تقنيات الحاسب الآلي من حيث برامجه , أنظمته , طبيعة الجريمة الواقعة عليه ومفرداتها من احتيال اليكتروني وقرصنة واختراق وحماية ، وكيفية كسر جدار الحماية ، وفيروسات الكمبيوتر ، ونظم استعمال ، ومعلومات دولية وغيرها من مصطلحات يمكنه عن طريقها التعامل مع هذه الجريمة المتفردة في خصوصيتها وكذلك التعامل مع المجرم المعلوماتي وهو مجرم ذو طبيعة خاصة يتعين تفهم كيفية التعامل معه.
- **البرنامج التدريبي:** يشتمل على الجانب النظري والعملي على النحو التالي (حجازي 2002م):
  - المخاطر والتهديدات وأماكن الاختراق لشبكة المعلومات وأجهزة الحاسب التي يمكن تعرضه لها.
  - مفاهيم معالجة البيانات, سواء ما تعلق بالبرامج أو الأجهزة.
  - نوعيات الجريمة المعلوماتية.
- **أسلوب أو منهج التحقيق من حيث مواده وهي:**
  - إجراءات التحقيق.
  - خطة التحقيق.
  - كيفية تجميع المعلومات وعرضها "استدلالات".
  - المواجهة والاستجواب.
  - النظم الفنية للبيانات.
  - طريقة عمل المختبر الجنائي
  - أسلوب عرض ودراسة الحالة.

ويضاف إلى ذلك موضوعات أخرى مثل التفتيش والضبط ، واستخدام الحاسب كوسيلة في الحصول على أدلة الاتهام ، والتعاون الدولي المشترك في ملاحقة هذه الجرائم.

وفي دراسة (بحر) أثبتت وجود معوقات فنية للتحقيق في جرائم الإنترنت حصرها فيما يلي: (1)

1. عدم كفاية المعرفة بالانجليزية.
2. عدم كفاية الخبرة للتحقيق في جرائم الانترنت.
3. عدم كفاية المعرفة لأساليب ارتكاب جرائم الانترنت.
4. عدم كفاية المعرفة لمصطلحات الانترنت.
5. عدم كفاية المعرفة لمصطلحات الحاسب.
6. عدم كفاية المهارات الفنية للتحقيق في جرائم الانترنت.
7. عدم كفاية المهارات الفنية للتحقيق في جرائم الحاسب.
8. عدم كفاية المعرفة لاستخدام الانترنت.
9. عدم كفاية المعرفة لاستخدام الحاسب.

7- أدوات التحقيق في الجرائم الإلكترونية :

- **برنامج التفتيش (Computer Search Warrant Program) :**

يسمح بإدخال كل المعلومات اللازمة لترقيم الأدلة وتسجيل البيانات عنها ، ويمكن لهذا البرنامج أن يصدر اتصالات باستلام الأدلة ، والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو ظروف ضبط هذا الدليل ، و يكون هذا البرنامج مع المحقق على قرص مرن أو قرص صلب محمول.

1- عبد الرحمن بحر (1999م) ، معوقات التحقيق في جرائم الانترنت ، "رسالة ماجستير غير منشورة " ، الرياض: جامعة نايف العربية للعلوم الأمنية.

- **قرص بدء تشغيل الحاسب (Bootable Diskette):**

يجب تأمين قرص بدء تشغيل الحاسب مع المحقق لتمكينه من تشـغيل الحاسـب إذا كان نظام التشغيل فيها محميا بكلمة مرور ، ويجب أن يكون القـرص مـزودا ببرنـامج مضاعفة المساحة (Double Space) فربما كان المتهم قد استخدم هذا البرنامج لمضـاعفة مساحة القرص الصلب.

- **برنامج (Xree Pro Cold) :**

وهو برنامج معالجة ملفات ممتاز يُمكِّن من العثور على الملفات في أي مكان علـى الشبكة ، أو على القرص الصلب ، ويستخدم لتقويم محتويات القـرص الصـلب الخـاص بالمتهم أو الأقراص المرنة المضبوطة. ويستخدم لقراءة البرامج في صورتها الأصلية ، كما يمكن استخدامه للبحث عن كلمات معينة أو عن أسماء ملفات أو غير ذلك مما لـه صـلة بالأمر.

- **برنامج (Lap Lkink) :**

وهو برنامج يمكن تشغيله من قرص مرن ، ويسمح بنسخ البيانات مـن الحاسـب الخاص بالمتهم ونقلها إلى قرص آخر من خلال المنفذ المتتالي (Serial Port) أو المنفـذ المتوازي (Parallel Port) وهذا البرنامج مفيد جداً للحصول على نسخة من المعلومـات قبل أي محاولة لتدميرها من جانب المتهم.

- **برنامج كشف الفيروسات وتدميرها :**

يمكن لأي برنامج من برامج مكافحة الفيروسات أن يؤدي إلى الغـرض ، وتكمـن أهمية مثل هذا البرنامج في ضمان حماية جهاز الحاسب الخاص بالمحقق.

- **برنامج (Ana Disk / View Disk):**

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المـرن مهمـا كـان أسلوب تهيئته. وهذا البرنامج توجد منه نسخة عادية تصلح للأفراد العاديين ونسخة خاصة

لرجال الشرطة أو محققي الحاسب الآلي. ويمكن الحصول عليه من شركة (Sydex Software).

- **برنامج الدمج وفك الدمج (Pkzip):**

وتستخدم لفك دمج البرامج ، فربما كان المتهم قد قام بدمج برامجه وفي هذه الحالة لا يمكن الاطلاع عليها إلا بعد فك الدمج.

- **برنامج اتصالات :**

مثل (Lantastic): وهوبرنامج يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات [1].

8- **التحقيق وخصوصية برمجياته :**

يستطيع خبراء الحاسوب والشبكات في فريق التحقيق فحص الحواسيب والشبكات بشكل دقيق وسريع ، بحثا عن أدلة رقمية وآثار سيبرانية يكون الجاني تركها وراءه ، كما يمكن من خلالها جمع المعلومات التي قد تكون ذات فائدة للتحقيق في هذه الجرائم. وهذه البرمجيات أهمها:

- برمجيات النسخ الاحتياطي الجنائي.
- برمجيات البحث عن المفردات النصية.
- برمجيات استعادة البيانات المحذوفة.
- برمجيات كسر كلمات سر بعض المستندات.
- برمجيات تتبع الاتصال الشبكي.
- برمجيات استعراض الصور.
- برمجيات عرض محتوي الملفات المختلفة.

1- حسن داود (2000م) ، جرائم نظم المعلومات ، الرياض: جامعة نايف العربية للعلوم الأمنية.

- برمجيات ضغط / فك ضغط الملفات.
- برمجيات استراق ضربات لوحة المفاتيح.

9- **مسرح الجريمة :**

من الممكن تحديد مراحل التعامل مع مسرح الجريمة عبر الخطوات التالية :(Wright, 2000) [1]

1- وضع الخطة.
2- حماية وتأمين مسرح الجريمة.
3- توثيق مخطط مسرح الجريمة.
4- البحث عن الأدلة.
5- إيجاد الأدلة.
6- معالجة الأدلة.

وربما كان الأمر الأكثر أهمية للمحقق فور وصوله إلى مسرح الجريمة هو السيطرة الكاملة على المنشآت والأشخاص في كافة حدود مسرح الجريمة والمناطق المحيطة به والتي من الممكن أن يطالها التفتيش ومن ثم يشرع في وضع خطة عمل دقيقة التفاصيل لجمع الأدلة تعتمد على نوعية التجهيزات الحاسوبية التي من المتوقع التعامل معها سواء على مستوى العتاد (Hard Ware) ، أو البرمجيات (Software) .

ويجب التعامل الحذر مع الأدلة الرقمية ، حيث يلزم أن يتم من خلال أيد خبيرة ومتخصصة في رفع وتحريز الأدلة الرقمية وعلى وجه الخصوص تلك الموجودة داخل أجهزة الحاسوب ، وبالذات تلك التي تكون قيد التشغيل وقت وصول فريق التحقيق إلى مسرح الجريمة (Wright, 2000a) ، ثم يترك المجال لخبراء التصوير سواء بالفيديو أو

1- Wright, Timothy(2000) (f). The Field Guide for Investigating Computer Crime, Part Six: Search and Seizure- Evidence Retrieval and Processing. [Online].

التصوير الفوتوغرافي لتصوير كامل الموقع بشكل دقيق يوضح موجوداته بشكلها الحالي قبل البدء الفعلي لعملية التفتيش (Vacca,2000) مع التأكيد على ضرورة أخذ صور فوتوغرافية لشاشات الحواسيب لتسجيل ما كانت تعرضه وقت جمع الأدلة ، والأخذ في الاعتبار أنه من الممكن أن يرتبط بجهاز حاسوب واحد أكثر من شاشة.

كما يجب أن يشمل التصوير الجهة الخلفية لأجهزة الحاسوب محل الفحص والأسلاك المرتبطة بها ، وأية ملحقات حاسوبية على اتصال مباشر بها ويشمل التصوير الجهة الخلفية لأجهزة الحاسوب محل الفحص ، والأسلاك المرتبطة بها ، وأية حاسوبية على اتصال مباشرة بها ، وكذلك عمل الخرائط التوضيحية (الكروكية) اللازمة لتحاكي وبدقة حال مسرح الجريمة وقت وصول فريق التحقيق له ، مع ضرورة أن يتأكد قائد الفريق من حرص جميع أعضاء فريق التحقيق على الأمور التالي بيانها أثناء تعاملهم مع الأدلة الرقمية على وجه الخصوص (Wright, 2000) : [(1)]

- عدم القيام بأي عمل من شأنه إحداث تعديل أو تغيير في أي دليل.
- عدم تنفيذ أية برامج على حواسيب في موقع الجريمة خصوصا البرامج ذات الصلة بأنظمة التشغيل.
- ضرورة عمل نسخ مطابقة للأقراص الصلبة ، ومن ثم عمل الفحوص الجنائية على هذه النسخ فقط ، سواء تم ذلك داخل مسرح الجريمة أو خارجه.

ولا تكفي نسخة احتياطية من البيانات المراد فحصها ، وإنما يجب عمل نسخة مطابقة تماما لكامل القرص الصلب ، إن مجرد مغادرة مسرح الجريمة يصبح من الصعب العثور على أية أدلة في حال قرر المحقق العودة إليه مرة أخرى لعمل ذلك.

أما أن تتم عملية فحص الحواسيب وجمع الأدلة الرقمية في مسرح الجريمة أو في المختبرات الجنائية ، فهذا قرار يجب أن يتخذه قائد فريق التحقيق بالتشاور مع خبير

1- Wright, Timothy(2000) (f). The Field Guide for Investigating Computer Crime, Part Six: Search and Seizure- Evidence Retrieval and Processing. [Online].

الحاسوب بناء على معطيات مسرح الجريمة وطبيعة الحواسيب محل الفحص ، ومدى الأهمية للجهة المتضررة بالإضافة إلى كم الأدلة المطلوب فحصها وطبيعتها.

1- أماكن وجود الأدلة الجنائية :

1- العتاد (Hardware): كأجهزة الحاسوب بأنواعها المختلفة والأقراص الصلبة الخارجية ، والملحقات المرتبطة بالحواسيب ذات الصلة بالجريمة كالطابعات والماسحات الضوئية والكاميرات الرقمية المودمات .. الخ.
2- البرمجيات (Software): إذا كان الدليل الرقمي نشأ باستخدام برنامج خاص أو ليس واسع الانتشار فإن أخذ الأقراص الخاصة بتنصيب هذا البرنامج أمر قد يكون في غاية الأهمية عند فحص هذا الدليل.
3- ملحقات الحاسوب: وتتمثل في المودم ، فقد تحوي فاكسات أو إمكانية الرد الآلي على المكالمات الهاتفية ، والطابعات التي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها.
4- وسائط التخزين المتحركة: هناك العديد منها والتي يمكن أن تحوي أدلة رقمية مثل: الأقراص المدمجة ، والأقراص المرنة ، الأشرطة المغناطيسية وأياً من الأشكال المختلفة لأشرطة تخزين البيانات الخارجية مثل الفلاش (Flash Memory).
5- المراشد (Manuals) الخاصة بالعتاد أو البرمجيات التي قد تفيد في معرفة التفاصيل الدقيقة لكيفية عملها وكذلك مجلات الحاسوب والأوراق المطبوعة [1].
6- كلمات السر أو أرقام الهاتف التي قد تكون مكتوبة على أوراق ملصقة بالحواسيب أو بقربها التي قد تكون خاصة بحسابات الاتصال بشبكة الإنترنت أو بعض

1- محمد الأمين البشرى (1421هـ) ، "التحقيق في جرائم الحاسب الآلي والانترنت" ، المجلة العربية للدراسات الأمنية والتدريب" س15 ، ع30 ، ص380-317 ، الرياض: جامعة نايف العربية للعلوم الأمنية.

خدمات الإنترنت المختلفة وربما كانت خاصة بفك تشفير بعض البيانات التي قد تحوي أدلة تفيد القضية.

7- البحث في سلة المهملات عن أوراق مطبوعة ذات علاقة بالحاسوب محل الفحص ، فقد تكون مفيدة خاصة إذا تطابقت مع النسخ الرقمية لبعض المعلومات على الحاسوب.

كما أن هنالك العديد من ملفات الولوج (Log Files) التي تحتوي على كمية هائلة من المعلومات عن الاستخدام الشخصي للكمبيوتر وهي بذلك مصدر من أهم المصادر للأدلة الرقمية ، ويرجع السبب في ذلك إلى ما يلي:

- تحتوي هذه الملفات على عناوين (IP) التي تمكن أجهزة البحث من تحديد أي كمبيوتر بالضبط ، قام بالفعل الإجرامي في الوقت المحدد المسجل وفي المكان المحدد المسجل ، وتفسير ذلك أن جهاز خادم الولوج (Server Log) يسجل كافة العناوين والتوقيتات والأزمنة للأجهزة المتصلة به ويشمل ذلك كافة الأنشطة المعلوماتية التي تتم على الشبكة مثل التصفح واستعراض المواقع المختلفة وإرسال واستقبال الرسائل الإلكترونية.
- ترتبط ملفات الولوج (Log Files) غالباً مع برامج الحماية Firewalls وبرامج تحديد المسارات (Routers) حيث تسجل غالباً تحركات الدخول والخروج مع بروتوكولات (TCP/IP) ويلاحظ أن صعوبة البحث هنا ، ترجع إلى أن ملفات الولوج في نظام (UNIX) تتطلب من رجال البحث الجنائي إلماماً خاصاً بطرق استخراج المعلومات ، حيث إن إعطاء بعض الأوامر دون البعض الآخر من شأنه أن يظهر بعض المعلومات دون البعض الآخر ، لذلك يجب على رجال البحث استخدام أوامر Syslog-Log-Var-More ، لاستخراج كافة المعلومات المسجلة عن النشاط الذي تم باستخدام جهاز الكمبيوتر [1].

1- ممدوح عبد المطلب (2003م) ، في بحث وتحقيق الجرائم على الكمبيوتر ، (د.م:د.ن).

2- المراقبة الإلكترونية :

تعد المراقبة من أهم مصادر التحري التي غالباً ما يستعان بها في البحث والتقصي عن الجرائم الإلكترونية ، فهي جزء لا يستغنى عنه في أعمال رجال البحث والتحري.

3- أهمية المعاينة في جرائم الإنترنت :

لا تتمتع المعاينة في مجال الكشف عن جرائم الإنترنت ، بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية ، ومرد ذلك إلى أن:

- الجرائم التي تقع على شبكة الشبكات أو بواسطتها قلَّما يترتب على ارتكابها آثار مادية.
- الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الزمنية والتي غالبا ما تكون طويلة نسبياً ما بين اقتراف الجريمة والكشف عنها ، الأمر الذي يتيح فرصة لحدوث تغيير أو تلفيق أو عبث بآثار الجريمة أو زوال بعضها وهو ما يلقي ظلالا من الشك على الدليل المستقى من المعاينة.
- إمكانية التلاعب في البيانات عن بعد ، أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل الجاني.

4- الاستجواب :

يجب إلمام المحقق في هذه الجرائم بمبادئ الحاسوب والإنترنت والمصطلحات المتعلقة بها. بالإضافة إلى معرفته بجرائم الحاسوب والإنترنت المختلفة وطرق ارتكابها ، ومبادئ وأسس أمن المعلومات بالشكل الذي يمكنه من التواصل الجيد مع الشهود والمتهمين من جهة ومع خبير الحاسوب في فريق التحقيق من جهة أخرى.

أما القواعد المتبعة في المناقشة والاستجواب فتكاد تكون واحدة في ما يتعلق بضرورة عزل الشهود والمتهمين حتى لا يتأثر أحدهم بأقوال الآخر أو يؤثر عليه ، وكذلك في الترتيب الذي يتم بموجبه أخذ الأقوال وأيضا في ضرورة أن يكون المحقق قادراً على

قراءة لغة الجسم ، ونبرة الصوت ، اللتين يستطيع من خلالهما معرفة ما إذا كان الشـــخص يقول الحقيقة أم لا.

وربما كان الأسلوب الأمثل في عملية الاستجواب هو الذي يقــوم علـــى ضـــرورة حضور خبير الحاسوب لعملية الاستجواب وتمكينه من الاشتراك فيهـــا بتوجيـــه الأســـئلة الفرعية للشاهد أو المتهم ، وربما قام بكتابة السؤال على قطعة من الورق ووضـــعها أمـــام المحقق ليقوم الأخير بتحَّين الفرصة المناسبة لإلقاء السؤال بما يتناسب والأصـــول الفنيـــة للاستجواب [1].

5- التحري :

ويفترض في الإجراءات السليمة للتحري أن تسهم في مساعدة فريق التحقيق على ما يلي:

- التثبت من وقوع الجريمة.
- تحديد نمط الجريمة المرتكبة وطبيعتها.
- التعرف على التقنيات المستخدمة في ارتكابها.
- المساعدة في تحديد الجاني أو الجناة المحتملين أو المشتبه بهم.
- معرفة الأسباب والدوافع المحتملة لارتكاب الجريمة.
- الاستدلال على الشهود في حالة وجودهم.
- توضيح طبيعة الأدلة الجنائية ومصادرها.

ويجب الأخذ في الاعتبار سرعة القيام بالتحريات في الفضـــاء الســـيبراني وذلـــك للطبيعة التي تختص بها الإنترنت من سرعة تغيّر المعلومات وزوالها ، حيث إن كـــل مـــا

1- محمد الأمين البشرى (1421هـ) ، "التحقيق في جرائم الحاسب الآلي والانترنـــت" ، المجلـــة العربيـــة للدراسات الأمنية والتدريب" س15 ، ع30 ، ص380-317 ، الرياض: جامعة نايف العربيـــة للعلـــوم الأمنية.

يكتب في منتديات الانترنت لا يتم الاحتفاظ به لفترات طويلة ، وحتى لو تم ذلـك يمكـن لفريق التحقيق أن يستخدم بعض الأدوات البرمجية في إجـراء التحريـات فـي الفضـاء السيبراني ، مثل برامج تتبع مصدر الاتصال الشبكي (Back Tracing) ، ومنها برنامج (Visual Route) وهذه العملية تشبه تتبع آثار أقدام المشتبه به في الجرائم التقليدية ، غير أنها تتم في دروب الفضاء السيبراني ، حيث يتم تتبع الطريق الـذي سـلكه المشـتبه بـه للوصول إلى الحاسوب أو الشبكة المتضررة.

ونظرا لما تكتنفه هذه البيئة من تعقيد وإشكاليات نقترح ما يلي:

- تشجيع المجني عليهم على الإبلاغ عن هذه الجرائم فوراً.
- حث العاملين على معاونة السلطة لضبط البيانات.
- ضرورة اتباع القواعد الفنية اللازمة لحماية البيانات وتجنيبها خطر الإتلاف.
- منح أوسع الصلاحيات لسلطة اختراق نظام الكمبيوتر وضبط ما يحويه التحقيق من بيانات مخزنة دون إخطار مسبق بعملية التفتيش والضبط.

10- **النتائج والتوصيات :**

نخلص من هذا البحث إلى نتائج وتوصيات عدة من أهمها:

أولاً- النتائج :

- إن مخاطر تصاعد وتيرة الجرائم الإلكترونية وتـداعياتها الاقتصـادية والجنائيـة والأخلاقية يجعل هذه القضية من كبرى القضايا الأمنية في وقتنا الحاضر ، فعليـه نوصي بدراسة هذه الظاهرة دراسة مستفيضة من قبل الجهات المعنية كافة.
- هناك مواكبة حثيثة لاقتناء التقنية المعلوماتية في المملكة والاستفادة منهـا تواكبهـا أيضا جهود وقائية من الجرائم تتمثل في صدور الأنظمة والتشريعات والدور المنوط بمدينة الملك عبد العزيز للعلوم والتقنية.
- في مجال التحقيق في الجرائم الالكترونية هناك بعض المعوقات التي تعترض الأداء المهني التقني الرفيع.

ثانياً – التوصيات:

- إجراء الدراسات الميدانية عن حجم الآثار والمشكلات الاقتصادية والمالية والاجتماعية والأمنية وغيرها الناشئة عن الجريمة الالكترونية.
- السعي إلى الاستفادة من الكفاءات العلمية والتقنية المتميزة في مجالات الأمن والادعاء العام والقضاء.
- تعميم مقرر مادة التحقيق في الجرائم الالكترونية وتشريعاتها "في المدارس والكليات الأمنية".
- بث الوعي الأمني لدى الجمهور عن مخاطر الجريمة الالكترونية.
- انتقاء ذوي المواهب والقدرات التقنية العالية للعمل في مجالات التحقيقات في الجرائم الإلكترونية.

المراجع

أولاً - المراجع العربية :

- خالد ممدوح إبراهيم (2009م) ، الجرائم المعلوماتية ، دار الفكر الجامعي.
- عبد الرحمن بحر (1999م) ، معوقات التحقيق في جرائم الانترنت ، "رسالة ماجستير غير منشورة " ، الرياض: جامعة نايف العربية للعلوم الأمنية.
- محمد الأمين البشرى (1423هـ) ، "الأدلة الجنائية الرقمية ودورها في الإثبات" ، المجلة العربية للدراسات الأمنية والتدريب ، س17 ، ع 33 ، ص147-91, الرياض: جامعة نايف العربية للعلوم الأمنية.
- محمد الأمين البشرى (1421هـ) ، "التحقيق في جرائم الحاسب الآلي والانترنت" ، المجلة العربية للدراسات الأمنية والتدريب" س15 ، ع30 ، ص380-317 ، الرياض: جامعة نايف العربية للعلوم الأمنية.
- جريدة الرياض ، عدد 2007/8/14م.
- حسن داود (2000م) ، جرائم نظم المعلومات ، الرياض: جامعة نايف العربية للعلوم الأمنية.
- محمد السرحاني (2004م) ، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت ، الرياض: جامعة نايف العربية للعلوم الأمنية.

- محمد شفيق (1995م) ، الجريمة والمجتمع ، الإسكندرية: المكتب الجامعي الحديث.
- جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، بيروت: دار النهضة العربية.
- ممدوح عبد المطلب (2003م) ، في بحث وتحقيق الجرائم على الكمبيوتر ، (د.م:د.ن).
- عمر حسن عدس (1995م) ، جرائم الحاسب الآلي وأشكالها وأساليب مواجهتها ، "بحث مقدم لمؤتمر قادة الشرطة والأمن العرب ، 16ــ1995/10/18م) ، ص 109.
- سليمان العنزي (2003م). وسائل التحقيق في جرائم نظم المعلومات. "رسالة ماجستير غير منشورة" ، الرياض: أكاديمية نايف العربية للعلوم الأمنية, الرياض.
- محمد القاسم ورشيد الزهراني (1427هـ) ، نموذج مقترح للتعامل مع جرائم المعلوماتية بالمملكة العربية السعودية. مجلة البحوث الأمنية ، ع22 ربيع الأخر 1427هـ.
- نبيلة هروال (2006م) ، الجوانب الإجرائية لجرائم الانترنت ، بيروت: دار الفكر الجامعي.

ثانياً - الأجنبية :

- Denning, D.& Baugh, E.(1999).Hiding crime in Cyberspace. [online]Available.
- Furnell, Steven (2002) .Cybercrime: Vandalizing the information society Boston : Addison-Wesley
- Grimes, Roger(2001). Malicious Mobile Code. Sebastopol, California: O'Reilly & Associates.
- Hpze, Crooll (1981), White Crime, Butterworth, London.
- Stephenson, Peter(2000). Investigating Computer-Related Crime. Boca Raton, Florida: CRC Press.
- Wright, Timothy(2000) (f). The Field Guide for Investigating Computer Crime, Part Six: Search and Seizure- Evidence Retrieval and Processing. [Online]. Available: http://www.securityfocus.com/infocus/1249 [05-09-2003]

Cyber- Crimes Modern Investigative Techniques [1]

Major General Dr. Mohammed Hassan Alsara [2]

Assistant Prof- Police Sciences Section- College of Higher Studies

Naif Arab University for Security Sciences

Abstract

The study aims at probing the nature of cyber crimes; which are not only bizarre or thorny, but also a big challenge for the police, judiciary and public prosecution offices to address in terms of scientific and technological readiness. The study endeavors to highlight the nature and myriad forms of these crimes which are currently the most serious and sophisticated particularly in the security fields of electronic websites and personal details protection; trespassing on electronic money; electronic signature and electronic consumer protection ; national economy , etc. The study also sets forth risks facing the information system; ways of uplifting security and preventive measures without detriment to privacy protection and finally highlighting national preventive efforts. The study argues that improving investigative techniques and all procedures required to deal with such crimes hugely hinges on the application of training programs; benefiting from successful experiences in dealing with criminal evidences and catching up with latest developments. Notwithstanding the fact that dealing with such kind of crimes necessitates seeking assistance of IT experts to unveil the mystery of digital evidences, yet, police and public prosecution offices' independence in such matter has become professionally needed. The study concluded with a number of findings and recommendations; the most salient of which are that cyber crimes with their associated risks and wide range of implications are the most serious nowadays. In its recommendations, the study stresses the necessity for conducting exhaustive studies on cyber crimes by all concerned bodies. KSA is seeking persistently to catch up with the latest technologies, and prevention effort against cyber crimes are in full swing, a matter that can be manifested in the issuance of new legislations and determining the role of king Abdulaziz City for Sciences and Technology. However, cyber crimes investigation is hampered by a number of obstacles. Among the recommendations set forth by the study are also; benefiting from experts and scholars in the fields of security and judiciary; generalizing Cyber – Crime Investigation course in Arab schools and security institutions; raising security awareness to risks of cyber crimes among the people and lastly opting for those highly talented in IT to work in cyber crimes investigation fields.

Keywords: Cyber Crimes – Electronic Websites – Electronic Money – Electronic Evidences – Electronic Lab.

[1]-**Manuscript** was submitted in September 2012 (under the Number 2012\7New), refereed in October 2011 and approved for publication in February 2012.

[2]-**Biography:** Major General Mohammed Hassan attained his PhD in Planning, Organization and Administrative Policies from California University- USA in 1990, and worked previously at King Fahad Security College. He is currently an assistant professor at Police Sciences Section - Naif Arab University for Security Sciences. He contributed a great deal of researches and studies.